## FIG. 1

	1	
HOST		TERMINAL
RANDOM DATA (R1, R2, n)	STEP 10 R1, R2, n	RUN KEY GENERATE ALGORITHM Ks=ENCRYPT(R1, KT[n])
RUN KEY GENERATE ALGORITHM		
Ks=ENCRYPT(R1, KT[n]) S1h=SIG(R2,Ks)		
	STEP 12	RUN AUTHENTICATION ALGORITHM
	S1t, R3	S1t=SIG(R2,Ks) RANDOM DATA R3
IF (S1h==S1t) {		TANDOW DATA NO
TERMINAL AUTHENTICATED (GENERATE SIGNATURE VALUE)	STEP 14	
\$2h=Sig(H+ R3+EnAmnt, Ks)		
ELSE { AUTHENTICATION FAILED		S2t=SIG(H+R3+ENAMNT,Ks)
EXIT COMMUNICATION }		
		CHECK SIGNATURE
·		IF(S2h==S2t) { HOST AUTHENTICATED
		AMOUNT=DECRYPT(EnAmnt, Ks)   BALANCE=BALANCE+AMOUNT
	STEP 16 M	(STORE VALUE)
  BALANCE'+ID'=DECRYPT(M,Ks)		M=ENCRYPT(BALANCE+ID,Ks)
IF (ID'==ID) {		ELSE {
BACK UP BALANCE STORE BALANCE IN RECORD FILE		AUTHENTICATION FAILED
· }		}

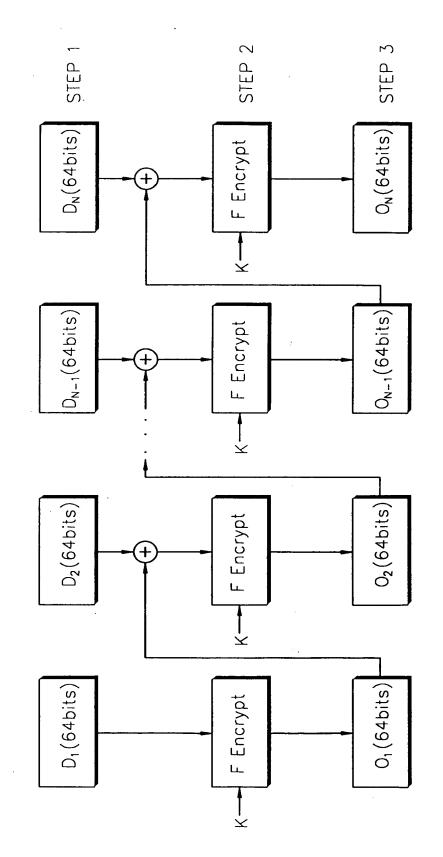
## FIG. 2

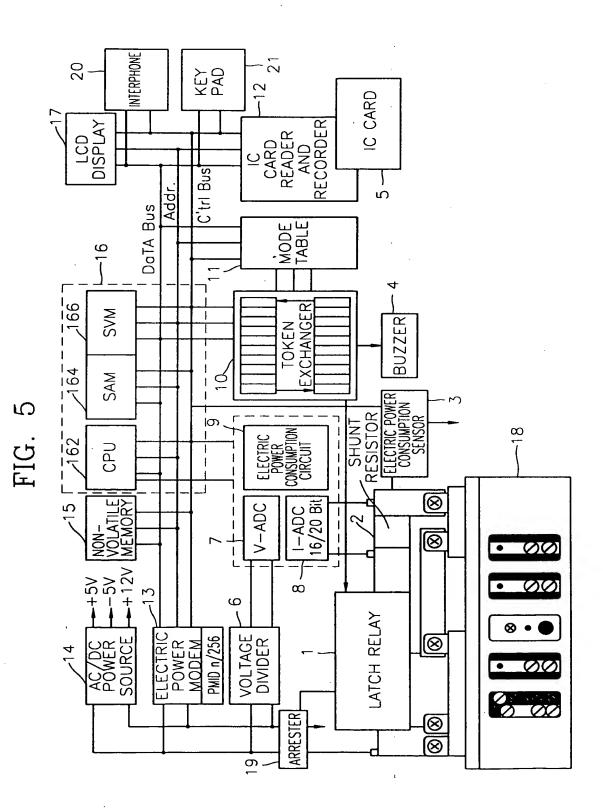
	1	
HOST		TERMINAL
RANDOM DATA (R1, R2, n)	STEP 20 R1, R2, n	RUN KEY GENERATE ALGORITHM KS=ENCRYPT(R1, KT[n])
RUN KEY GENERATE ALGORITHM Ks=ENCRYPT(R1, KT[n]) S1h=SIG(R2,Ks)		
	STÉP 22 S1t, R3	RUN AUTHENTICATION ALGORITHM S1t=SIG(R2,Ks) RANDOM DATA R3
IF (S1h==S1t) { TERMINAL AUTHENTICATED (GENERATE SIGNATURE VALUE) S2h=SIG(H+R3+MODE+UNIT,Ks) ELSE { AUTHENTICATION FAILED EXIT COMMUNICATION }	STEP 24 Mode+Unit, S2h	S2t=SIG(H+R3+MODE+UNIT,Ks)
	STEP 26	CHECK SIGNATURE IF(S2h==S2t) { HOST AUTHENTICATED CHANGE MODE (CONVERT RATE SYSTEM) M=ENCRYPT(BALANCE+ID,Ks) }
BALANCE'+ID'=DECRYPT(M,Ks) IF (ID'==ID) { BACK UP BALANCE STORE BALANCE IN RECORD FILE }		ELSE { AUTHENTICATION FAILED EXIT COMMUNICATION }

## FIG. 3

	1	
HOST		TERMINAL
RANDOM DATA (R1, R2, n)	STEP 30 R1, R2, n	RUN KEY GENERATE ALGORITHM Ks=ENCRYPT(R1, KT[n])
RUN KEY GENERATE ALGORITHM Ks=ENCRYPT(R1, KT[n]) S1h=SIG(R2,Ks)		
	STEP 32 S1t, R3	RUN AUTHENTICATION ALGORITHM S1t=SIG(R2,Ks) RANDOM DATA R3
IF (S1h==S1t) { TERMINAL AUTHENTICATED (GENERATE SIGNATURE VALUE) S2h=Sig(H+ R3+TIME,Ks) ELSE { AUTHENTICATION FAILED EXIT COMMUNICATION }	STEP 34 Time, S2h	S2t=Sig(H+R3+Time,Ks)
INFO'=DECRYPT(M,Ks) IF(ID'==ID) { STORE AND CHECK USE DURING DAYS, WEEKS, AND MONTHS AND TIMER INFORMATION }	STEP 36 M	CHECK SIGNATURE IF(S2h==S2t) { HOST AUTHENTICATED  INFO=LOG+MODE TB+TIMER+BALANCE+ID M=ENCRYPT(INFO, Ks) SET TIME (AMEND TIME) } ELSE { AUTHENTICATION FAILED EXIT COMMUNICATION }

FIG. 4





TRANSFER VALUE 53 54 HEATING ALL THE METERS EXCLUDING ELECTRICITY.OFF LINE 0 0 GAS AMOUNT OF MONEY CALCULATION SYSTEM ELECTRIC POWER SUPP<sub>I</sub>LIER TRANSFER 3.3kv 220V POWER SUPPLY SV+ICEPM SURSCRIBER FIFCTOR POWER/CAS/WATER MATER 0000 WATER LS2) TRANSFER VALUE SETTLE AMOUNT OF MONEY LS1) ONE CARD INCLUDES ELECTRIC POWER, WATER, HOT WATER, GAS, AND HEAT ENERCY ELECTRONIC PURSES, PSŤN 55-0 SVEPM 901 Max. 3Km ASIX (ASZ) -50 <u></u> **□** <del>| -5</del>2 LOCAL MANAGEMENT COMPUTER 0 ISSUE IC CARD 0 ELECTRIC POWER RE-SELLER-IC CARD ž ELECTRIC POWER RE-SELLER LS: LOCAL SERVICE & SURVEILLANCE AS; AREA SERVICE & SURVEILLANCE ARS BANK/CREDIT/ DIRECT PAYMENT/ CARD COMPANY ADVANCE PAYMENT

FIG. 6

FIG. 7

